

Kaseya 2

Data Backup

Benutzerhandbuch

Versión R8

Deutsch

Oktober 23, 2014

Agreement

The purchase and use of all Software and Services is subject to the Agreement as defined in Kaseya's "Click-Accept" EULATOS as updated from time to time by Kaseya at http://www.kaseya.com/legal.aspx. If Customer does not agree with the Agreement, please do not install, use or purchase any Software and Services from Kaseya as continued use of the Software or Services indicates Customer's acceptance of the Agreement."

Inhalt

Überblick über Data Backup

Data Backup (KDB) ist ein Addon-Modul, das ausgewählte Dateien und Ordner entweder in der Amazon S3-Cloud oder auf Ihrem eigenen privaten Speicherserver sichert. Private Speicherserver können lokal oder als private *Cloud*-Speicher konfiguriert werden. Der auf Amazon S3-Cloud basierende Backup-Service erspart Ihnen die Kosten und den Wartungsaufwand eigener Backup-Lösungen, die über entweder zu wenig oder zu viel Speicherkapazität verfügen. Die private Speicheroption auf der anderen Hand gibt Ihnen die Flexibilität, vorhandene Speicherinvestitionen auszunutzen.

Gebührenbasierte oder private Speicherlösungen

Für eine zusätzliche Gebühr können Sie die Dienste des Speicheranbieters Amazon S3 in Anspruch nehmen oder aber Ihre eigenen über einen Agent verwalteten Rechner als Speicher für Ihre Backups konfigurieren. Bei beiden Speicherlösungen gibt es keine Größenbeschränkungen für Dateien. Der private Speicherserver muss sich nicht im selben lokalen Netzwerk wie der zu sichernde Rechner befinden. Ein privater Speicherserver kann auf ein lokales Laufwerk oder einen UNC-Pfad zu einem externen Speicher wie beispielsweise einem NAS-Gerät verweisen. Sie brauchen nur einen DNS-Namen oder eine IP-Adresse, Portnummer sowie ein lokales Laufwerk und ein Ordnerverzeichnis anzugeben, um auf einen privaten Speicherserver zuzugreifen. Für private Speicherserver fallen keinen diesbezüglichen Lizenzgebühren an.

- Auf der Seite **Privater Speicher** *(siehe 18)* können Sie einen Rechner als privaten Speicher konfigurieren.
- Auf der Seite **Kaseya Cloud Storage** *(siehe 19)* können Sie den Amazon S3-Speicherserver aktivieren.

Cloud-Abrechnungsservice

Der **Data Backup**-Service wird gestartet und über den Kaseya Cloud-Abrechnungsservice in Rechnung gestellt. Abrechnungsinformationen können Sie auf dem **Kaseya Portal** *(http://portal.kaseya.net)* einsehen. Der Service umfasst Planungs- und Bandbreitenoptionen, die Backups während der Spitzenbelastungszeiten einschränken oder verhindern.

Aufbewahrungsrichtlinie

- Backup-Daten der letzten 30 Tage werden im Online-Speicher aufbewahrt.
- Inkrementelle Backups werden nur gespeichert, wenn seit der letzten Speicherung Änderungen vorgenommen worden sind.
- Nach Speicherung von jeweils 30 inkrementelle Backups erfolgt das darauffolgende Backup als Spiegel-Backup (vollständig).
- Wenn ein inkrementelles Backup 80 % oder mehr der Größe der gesicherten Datei erreicht, wird ein Spiegel-Backup (vollständig) erstellt.
- Wenn sich eine Datei seit mehr als 30 Tagen nicht geändert hat, wird nur ihre letzte Version aufbewahrt.
- Wenn eine Datei vom Agent gelöscht wird, wird die letzte Version zeitlich unbegrenzt extern gespeichert, es sei denn, sie wird mithilfe der Funktion **Verwalten** *(siehe 9)* gelöscht.
- Für sowohl Cloud- als auch private Speicherung gilt, dass, wenn **Data Backup** von einem Endpunkt deinstalliert wird, alle Backup-Daten dieses Endpunkts vom Speicherserver gelöscht werden.
- Für Cloud-Speicherung gilt, dass, wenn der Kaseya-Agent vor **Data Backup** vom einem Endpunkt deinstalliert wird, die Daten auf dem Amazon S3-Server verbleiben und *Ihnen die Nutzung weiterhin in Rechnung gestellt wird*.

Installieren/Entfernen

Über die Seite **Installieren/Entfernen** wird nichts auf dem zu sichernden Agent-Rechner installiert, sondern die Verwaltung dieses Rechners durch **Data Backup** ermöglicht. Die Installation ist erforderlich, damit die Rechner-ID auf anderen **Data Backup**-Seiten angezeigt wird.

Backup-Profile

Auf der Seite **Backup-Profile** können Sie Konfigurationsprofile für das Backup verwalten. Jedes Backup-Profil besteht aus einem unterschiedlichen Satz aktivierter bzw. deaktivierter Backup-Optionen, darunter die für das Backup vorgesehenen Dateitypen und Dateispeicherorte. Ein- und Ausschlussregeln können nach Dateityp definiert werden. **Dateien und Verzeichnisse werden entsprechend einer festen Rangfolge ein- bzw. ausgeschlossen.** *(siehe 15)*

Änderungen an einem Profil wirken sich auf alle Rechner-IDs aus, denen dieses Profil zugewiesen wurde. Normalerweise benötigen verschiedene Typen von Rechnern unterschiedliche Backup-Profile. Es wird Ihnen ein Musterprofil bereitgestellt. Dieses Musterprofil kann zwar nicht geändert werden, aber Sie können es unter einem neuen Namen speichern und dann Änderungen an der Kopie vornehmen. Zu den Backup-Profiloptionen gehören Performance-Optionen zur Bandbreiten- und CPU-Einschränkung.

Backup-Profile sind optional, aber sehr zu empfehlen. Bei der einzigen anderen Methode für die Planung eines Backups müssen Sie Dateien einzeln auf einem Rechner auswählen. Backup-Profile werden mit der Profilauswahl rechts oben auf der Seite **Planen** *(siehe 4)* einem Rechner-ID-Konto zugewiesen.

Profilvariablen

Geben Sie, wenn Sie Objekte in ein Profil einschließen bzw. davon ausschließen, ein Prozentzeichen (%) als erstes Zeichen ein, um eine Liste mit *Profilvariablen* anzuzeigen. Nicht alle Profilvariablen gelten für OSX-Betriebssysteme.

Erstellen von Backups

Auf der Seite **Planen** können Sie Backups erstellen.

1. Wählen Sie eine oder mehrere der Rechner-IDs aus.
2. Wählen Sie einen Speicherserver. Wenn Sie diese Funktion auf der Seite **Kaseya Cloud Storage** *(siehe 19)* aktiviert haben, steht auch ein Amazon S3-Speicherserver zur Wahl. Ein *privater Speicherserver* wird nur angezeigt, wenn Sie ihn auf der Seite **Privater Speicher** *(siehe 18)* als solchen konfiguriert haben.
3. Wählen Sie entweder **Backup-Profil**, **Dateiauswahl** oder beides aus. Sie müssen mindestens eine der beiden Optionen auswählen.
4. Klicken Sie auf **Planen** oder **Jetzt sichern**, um die Erstellung von Backups für ausgewählte Rechner-IDs zeitlich festzulegen bzw. sofort auszuführen.

Wiederherstellen von Backups

Auf der Seite **Wiederherstellen** können Sie ausgewählte Ordner und Dateien eines Backups entweder auf demselben Rechner, von dem das Backup erstellt wurde, oder auf einem anderen Rechner mit kompatiblem Betriebssystem wiederherstellen. Dateien mit demselben Namen können Sie wahlweise überschreiben oder Kopien davon erstellen. Darüber hinaus können Sie entscheiden, ob Sie die Dateien und Ordner an ihrem ursprünglichen oder an einem neuen Speicherort wiederherstellen möchten.

Meldungen

Die Seite **Meldungen** gibt in Reaktion auf erfolgreiche bzw. fehlgeschlagene **Data Backup**-Ereignisse Meldungen aus.

Speicherstatus

Mithilfe der folgenden Seiten und Berichte können Sie den Status von Speicherservern und Backups

verfolgen:

- **Status** *(siehe 4)*
- **Protokolle** *(siehe 7)*
- **Übersicht** *(siehe 10)*
- **Überblick** *(siehe 10)*
- **Datensicherung-Zusammenfassung** *(siehe 20)*
- **Datensicherungsnutzung im Zeitverlauf** *(siehe 20)*

Hinweis: Siehe Data Backup-Systemanforderungen.

Funktionen	Beschreibung
Status *(siehe 4)*	Zeigt eine Dashboard-Ansicht des Status aller Rechner-IDs an, auf denen Data Backup installiert ist.
Planen *(siehe 4)*	Legt Backups ausgewählter Rechner-IDs zeitlich fest.
Protokolle *(siehe 7)*	Zeigt Protokolle aller in den letzten 90 Tagen ausgeführten Backups und Wiederherstellungen an.
Wiederherstellen *(siehe 7)*	Stellt ausgewählte Ordner und Dateien eines Backups auf einer ausgewählten Rechner-ID wieder her.
Verwalten *(siehe 9)*	Ermöglicht das Löschen von Ordnern und Dateien aus einem Backup einer ausgewählten Rechner-ID.
Übersicht *(siehe 10)*	Zeigt Speicherstatistiken der einzelnen gesicherten Rechner-IDs an.
Überblick *(siehe 10)*	Zeigt Speicherstatistiken zuerst gruppiert nach privaten Speicherservern, dann nach Rechner-ID an.
Installieren/Entfernen *(siehe 11)*	Aktiviert Data Backup auf ausgewählten Rechner-IDs bzw. deinstalliert Data Backup davon.
Backup-Profile *(siehe 12)*	Definiert Backup-Konfigurationsprofile.
Meldungen *(siehe 16)*	Definiert Meldungen zu Backup-Ereignissen.
Privater Speicher *(siehe 18)*	Konfiguriert verwaltete Rechner als private Speicherserver.
Kaseya Cloud Storage *(siehe 19)*	Aktiviert die Speicherung in der Amazon S3-Cloud.

Data Backup-Modulanforderungen

Kaseya Server

- Das Data Backup R8-Modul setzt VSA R8 voraus.

Anforderungen für verwaltete Rechner

- Microsoft Windows Server 2003, 2003 R2, 2008, 2008 R2, 2012, 2012 R2
- Microsoft Windows XP, Vista, 7, 8, 8.1
- Apple OS X 10.5 bis 10.9 – nur Intel

Anforderungen für private Speicherserver

- Microsoft Windows XP, Vista, 7, 8
- Microsoft Windows Server 2003, 2003 R2, 2008, 2008 R2, 2012
- Auf einem privaten Speicherserver muss ein Agent installiert sein.

- Achten Sie darauf, dass auf dem privaten Speicherserver ausreichend Speicherplatz vorhanden ist, um die Speicheranforderungen des Endpunkts zu erfüllen.

> **Hinweis:** Siehe allgemeine **Systemanforderungen** *(http://help.kaseya.com/webhelp/DE/VSA/R8/reqs/index.asp#home.htm)*.

Status

Data Backup > Backup > Status

Die Seite **Status** bietet eine Dashboard-Ansicht des Status von gesicherten Rechnern.

Der Bereich **Backup-Status** zeigt abgeschlossene, mit Ausnahmen abgeschlossene, übersprungene, fehlgeschlagene, teilweise fehlgeschlagene, laufende und nicht geplante Backups als Kreisdiagramm an. Ein teilweise fehlgeschlagenes Backup bedeutet, dass einige Dateien möglicherweise nicht gesichert werden konnten. Klicken Sie auf ein Segment oder eine Bezeichnung des Kreisdiagramms, um eine Liste der einzelnen Rechner anzuzeigen, die zu diesem Segment gehören.

> **Hinweis:** Backups werden möglicherweise `übersprungen`, wenn die Verbindung vorübergehend unterbrochen war. `Mit Ausnahmen abgeschlossen` weist auf ein möglicherweise kritisches Problem des Backups hin. In beiden Fällen wird eine Beschreibung des Problems auf den Seiten **Status** und **Protokolle** *(siehe 7)* angezeigt.

Statistiken können auf zwei Weisen gefiltert werden:

- **Backup-Status für letzte/s/n <N> <Perioden>** – Begrenzt die Statistik auf den ausgewählten Zeitraum.
- **Rechner-ID/Gruppen-ID-Filter** – Begrenzt die Statistik auf die durch den Rechner-ID/Gruppen-ID-Filter bestimmten Backup-Rechner.

  > **Hinweis:** Rechner-IDs werden auf dieser Seite nur angezeigt, wenn **Data Backup** darauf **installiert** *(siehe 11)* ist. Die Liste der auswählbaren Rechner-IDs basiert auf dem Rechner-ID-/Gruppen-ID-Filter und dem verwendeten Scope.

Klicken Sie auf die mit Hyperlink verknüpften Zahlen (nicht null) in der Spalte **Übersprungen**, um die Einträge auf der Seite **Protokolle** *(siehe 7)* für die einzelnen Rechner anzuzeigen.

Planen

Data Backup > Backup > Planen

Auf der Seite **Planen** können Sie Backups ausgewählter Rechner-IDs zeitlich festlegen.

1. Wählen Sie eine oder mehrere der Rechner-IDs aus.
2. Wählen Sie einen Speicherserver. Wenn Sie diese Funktion auf der Seite **Kaseya Cloud Storage** *(siehe 19)* aktiviert haben, steht auch ein Amazon S3-Speicherserver zur Wahl. Ein *privater Speicherserver* wird nur angezeigt, wenn Sie ihn auf der Seite **Privater Speicher** *(siehe 18)* als solchen konfiguriert haben.
3. Wählen Sie entweder **Backup-Profil**, **Dateiauswahl** oder beides aus. Sie müssen mindestens eine der beiden Optionen auswählen.
4. Klicken Sie auf **Planen** oder **Jetzt sichern**, um die Erstellung von Backups für ausgewählte Rechner-IDs zeitlich festzulegen bzw. sofort auszuführen.

> **Hinweis:** Rechner-IDs werden auf dieser Seite nur angezeigt, wenn **Data Backup** darauf **installiert** *(siehe 11)* ist. Die Liste der auswählbaren Rechner-IDs basiert auf dem Rechner-ID-/Gruppen-ID-Filter und dem verwendeten Scope.

Aufbewahrungsrichtlinie

- Backup-Daten der letzten 30 Tage werden im Online-Speicher aufbewahrt.
- Inkrementelle Backups werden nur gespeichert, wenn seit der letzten Speicherung Änderungen vorgenommen worden sind.
- Nach Speicherung von jeweils 30 inkrementelle Backups erfolgt das darauffolgende Backup als Spiegel-Backup (vollständig).
- Wenn ein inkrementelles Backup 80 % oder mehr der Größe der gesicherten Datei erreicht, wird ein Spiegel-Backup (vollständig) erstellt.
- Wenn sich eine Datei seit mehr als 30 Tagen nicht geändert hat, wird nur ihre letzte Version aufbewahrt.
- Wenn eine Datei vom Agent gelöscht wird, wird die letzte Version zeitlich unbegrenzt extern gespeichert, es sei denn, sie wird mithilfe der Funktion **Verwalten** *(siehe 9)* gelöscht.
- Für sowohl Cloud- als auch private Speicherung gilt, dass, wenn **Data Backup** von einem Endpunkt deinstalliert wird, alle Backup-Daten dieses Endpunkts vom Speicherserver gelöscht werden.
- Für Cloud-Speicherung gilt, dass, wenn der Kaseya-Agent vor **Data Backup** vom einem Endpunkt deinstalliert wird, die Daten auf dem Amazon S3-Server verbleiben und *Ihnen die Nutzung weiterhin in Rechnung gestellt wird*.

Aktionen

- **Planen** – Klicken Sie auf **Planen**, um das Fenster **Planer** einzublenden, das im gesamten VSA zur Planung von Aufgaben verwendet wird. Planen Sie die einmalige oder periodische Ausführung einer Aufgabe. Jede Art von Wiederholung (fortlaufend, einmal, minütlich, stündlich, täglich, wöchentlich, monatlich) zeigt weitere Optionen für diese Art von Wiederholung an. Periodische Zeitplanung bedeutet, dass Sie Start- und Endtermine für die Wiederholung einstellen müssen. Nicht alle Optionen stehen für jede geplante Aufgabe zur Verfügung. Optionen können Folgendes umfassen:
  - **Fortlaufend** – Geänderte Dateien werden innerhalb von 10 Minuten gesichert. Neue Dateien werden innerhalb von 24 Stunden gesichert.
  - **Verteilungsfenster** – Plant die Aufgabe zu einem willkürlichen Zeitpunkt neu (nicht später als die angegebene Anzahl von Perioden), um den Datenverkehr und die Serverlast zu verteilen. Beispiel: Wenn die Ausführung einer Aufgabe für 3:00 Uhr geplant ist und das Verteilungsfenster 1 Stunde beträgt, wird die Zeitplanung für die Aufgabe in einen zufälligen Zeitpunkt zwischen 3:00 und 4:00 Uhr geändert.
  - **Überspringen, wenn offline** – Falls dies aktiviert und der Rechner offline ist, wird dies übergangen und zur nächsten geplanten Uhrzeit ausgeführt. Wenn diese Option leer gelassen wird und der Rechner offline ist, führen Sie die Aufgabe aus, sobald der Rechner wieder online ist.
  - **Bei offline einschalten** – Nur Windows. Wenn dies aktiviert ist, wird der Rechner hochgefahren, falls er offline ist. Erfordert Wake-On-LAN oder vPro und ein anderes verwaltetes System auf dem gleichen LAN.
  - **Folgenden Zeitrahmen ausschließen** – **Bezieht sich ausschließlich auf das Verteilungsfenster.** Falls markiert, wird ein Zeitrahmen im Verteilungsfenster angegeben, in dem die Aufgabe nicht geplant werden kann. Zeitangaben außerhalb des Verteilungsfensters werden ignoriert.
- **Jetzt sichern** – Legt ein Backup für die sofortige Ausführung fest.
- **Abbrechen** – Löscht anstehende Backups ausgewählter Rechner-IDs, aber bricht keine bereits begonnenen Backups ab.

- **Speicherserver anwenden** – Wählen Sie einen Speicherserver aus, der für ausgewählte Rechner-IDs angewendet werden soll.
  - Ein privater Speicherserver wird nur angezeigt, wenn Sie ihn auf der Seite **Privater Speicher** *(siehe 18)* als solchen konfiguriert haben.
  - Der Amazon S3-Speicherserver wird angezeigt, wenn Sie diese Funktion auf der Seite **Kaseya Cloud Storage** *(siehe 19)* aktiviert haben.
- **Profil anwenden** – Wählen Sie ein Profil aus, das auf ausgewählte Rechner-IDs angewendet werden soll.

> **Hinweis:** Zur Auswahl der zu sichernden Ordner und Dateien müssen Sie entweder ein Backup-Profil anwenden, eine manuelle Auswahl vornehmen oder beides.

- **Entfernen** – Entfernen Sie ein Profil, eine Dateiauswahl oder beides von ausgewählten Rechner-IDs.

Rechner-ID

Die Liste der angezeigten Rechner-IDs basiert auf dem Rechner-ID-/Gruppen-ID-Filter und den Rechnergruppen, zu deren Ansicht über 'System > Benutzersicherheit > Scopes' der Benutzer berechtigt ist. Rechner-IDs werden auf dieser Seite nur angezeigt, wenn die Backup-Lösung darauf **installiert** *(siehe 11)* ist.

Check-in-Status

Diese Symbole geben den Agent-Anmeldestatus jedes verwalteten Rechners an. Wenn Sie den Cursor über ein Anmeldesymbol bewegen, wird das Agent-Quick View-Fenster angezeigt.

- Online, aber in Wartestellung bis zum Abschluss des ersten Audits
- Agent online
- Agent online und Benutzer gegenwärtig angemeldet.
- Agent online und Benutzer gegenwärtig angemeldet, doch Benutzer seit mehr als 10 Minuten nicht aktiv
- Agent ist gegenwärtig offline
- Agent hat nie eingecheckt.
- Agent ist online, aber die Fernsteuerung wurde deaktiviert.
- Agent wurde ausgesetzt.

Backup-Profil

Das dieser Rechner-ID zugewiesene **Backup-Profil** *(siehe 12)*

Speicherserver

Der dieser Rechner-ID zugewiesene Speicherserver

Dateiauswahl

Um Ordner und Dateien auszuwählen, die nicht im Backup-Profil eingeschlossen sind, klicken Sie auf das Symbol für die **Dateiauswahl** einer Rechner-ID. **Dateien und Verzeichnisse werden entsprechend einer festen Rangfolge ein- bzw. ausgeschlossen.** *(siehe 15)*

Wiederholung

Zeigt an, ob ein Backup geplant ist und ob es regelmäßig wiederholt wird. Ist eine Wiederholung geplant, wird das Wiederholungsmuster angegeben.

Nächstes Backup

Zeigt das geplante Datum und die geplante Uhrzeit des nächsten Backups an. Datum-/Zeitstempel für überfällige Vorgänge werden als roter Text mit gelber Hervorhebung angezeigt.

Protokolle

Data Backup > Backup > Protokolle

Auf der Seite **Protokolle** wird eine Liste aller in den letzten 90 Tagen ausgeführten Backups angezeigt. Klicken Sie auf eine Rechner-ID, um ein Protokoll mit Uhrzeit, Datum, Dauer, Ergebnis und Anzahl der Ausnahmen anzuzeigen.

Die Ergebnisse werden in der Spalte **Ergebnisse** angezeigt.

- `Übersprungen` – Backups werden möglicherweise übersprungen, wenn die Verbindung vorübergehend unterbrochen war.
- `Abgebrochen` – Das Backup wurde abgebrochen.

Wenn Sie bei einem der folgenden Ergebnisse auf den Link klicken, erhalten Sie zusätzliche Informationen dazu.

- `Mit Ausnahmen abgeschlossen` – Weist auf ein kritisches Problem bei der Backup-Erstellung hin.
- `Abgeschlossen` – Zeigt eine Liste mit gesicherten Dateien und nicht veränderten Dateien an, bei denen kein Backup erforderlich war.
- `Teilweise fehlgeschlagen` – Zeigt die Dateien an, die möglicherweise nicht erfolgreich gesichert werden konnten.

> **Hinweis:** Rechner-IDs werden auf dieser Seite nur angezeigt, wenn **Data Backup** darauf **installiert** *(siehe 11)* ist. Die Liste der auswählbaren Rechner-IDs basiert auf dem Rechner-ID-/Gruppen-ID-Filter und dem verwendeten Scope.

Wiederherstellen

Data Backup > Wiederherstellung > Wiederherstellen

Auf der Seite **Wiederherstellen** können Sie ausgewählte Ordner und Dateien eines Backups entweder auf demselben Rechner, von dem das Backup erstellt wurde, oder auf einem anderen Rechner mit kompatiblem Betriebssystem wiederherstellen. Dateien mit demselben Namen können Sie wahlweise überschreiben oder Kopien davon erstellen. Darüber hinaus können Sie entscheiden, ob Sie die Dateien und Ordner an ihrem ursprünglichen oder an einem neuen Speicherort wiederherstellen möchten.

> **Hinweis:** Wiederherstellungen werden möglicherweise **übersprungen**, wenn die Verbindung vorübergehend unterbrochen war. **Mit Ausnahmen abgeschlossen** – Weist auf ein möglicherweise kritisches Problem bei der Wiederherstellung hin. In beiden Fällen wird eine Beschreibung des Problems auf der Seite **Protokolle** *(siehe 7)* angezeigt.
>
> **Hinweis:** Rechner-IDs werden auf dieser Seite nur angezeigt, wenn **Data Backup** darauf **installiert** *(siehe 11)* ist. Die Liste der auswählbaren Rechner-IDs basiert auf dem Rechner-ID-/Gruppen-ID-Filter und dem verwendeten Scope.

Aufbewahrungsrichtlinie

- Backup-Daten der letzten 30 Tage werden im Online-Speicher aufbewahrt.
- Inkrementelle Backups werden nur gespeichert, wenn seit der letzten Speicherung Änderungen vorgenommen worden sind.
- Nach Speicherung von jeweils 30 inkrementelle Backups erfolgt das darauffolgende Backup als Spiegel-Backup (vollständig).

- Wenn ein inkrementelles Backup 80 % oder mehr der Größe der gesicherten Datei erreicht, wird ein Spiegel-Backup (vollständig) erstellt.
- Wenn sich eine Datei seit mehr als 30 Tagen nicht geändert hat, wird nur ihre letzte Version aufbewahrt.
- Wenn eine Datei vom Agent gelöscht wird, wird die letzte Version zeitlich unbegrenzt extern gespeichert, es sei denn, sie wird mithilfe der Funktion **Verwalten** *(siehe 9)* gelöscht.
- Für sowohl Cloud- als auch private Speicherung gilt, dass, wenn **Data Backup** von einem Endpunkt deinstalliert wird, alle Backup-Daten dieses Endpunkts vom Speicherserver gelöscht werden.
- Für Cloud-Speicherung gilt, dass, wenn der Kaseya-Agent vor **Data Backup** vom einem Endpunkt deinstalliert wird, die Daten auf dem Amazon S3-Server verbleiben und *Ihnen die Nutzung weiterhin in Rechnung gestellt wird*.

Wiederherstellungsstatus

Der Wiederherstellungsstatus einer Rechner-ID lässt sich anhand von Symbolen und daran ablesen, ob Text aktiviert oder deaktiviert ist.

– Für diese Rechner-ID sind keine Backup-Dateien vorhanden. Der Name der Rechner-ID wird in *grauer Kursivschrift* angezeigt

– Backupdateien sind vorhanden und können auf dieser Rechner-ID oder auf einem anderen Rechner mit kompatiblem Betriebssystem wiederhergestellt werden. Der Name der Rechner-ID wird als *aktivierter Text* angezeigt.

– Backupdateien sind vorhanden, aber der Rechner ist offline. Die Backupdateien können nur auf einem *anderen* Rechner wiederhergestellt werden.

Wiederherstellung eines Backups von einem *Online*-Rechner

1. Wählen Sie im mittleren Bereich der Seite 'Data Backup > **Wiederherstellen**' eine Rechner-ID mit einem -Symbol und *aktiviertem Text* aus.
2. Wählen Sie in der Dropdown-Liste **Backup-Instanz auswählen** Datum und Uhrzeit eines vorhandenen Backups aus.
3. Klicken Sie auf **Arbeitsplatz**, um die Ordnerstruktur zu erweitern. Die Ordnerstruktur enthält die Ordner und Dateien, die Bestandteil der ausgewählten Backup-Instanz sind.
4. Wählen Sie die Ordner und Dateien aus, die Sie wiederherstellen möchten.
5. Markieren Sie gegebenenfalls die Option **Vorhandene Dateien überschreiben**.
6. Wählen Sie mit **Wiederherstellen auf** den Speicherort auf dem *ursprünglichen* Rechner aus, auf dem das Backup wiederhergestellt werden soll. Wenn Sie dieses Feld leer lassen, werden die Dateien an ihrem ursprünglichen Speicherort wiederhergestellt. Auf Wunsch können Sie ein anderes Zielverzeichnis auf dem ursprünglichen Rechner auswählen. UNC-Pfade werden nicht unterstützt. Nach Angabe des Speicherortes können Sie unter folgenden Optionen auswählen:
   - **Datei ersetzen, wenn vorhanden** – Wenn am angegebenen Zielspeicherort eine Version der wiederherzustellenden Datei vorhanden ist, wird sie mit der wiederhergestellten Datei überschrieben.
   - **Datei umbenennen, wenn vorhanden** – Wenn am angegebenen Zielspeicherort eine Version der wiederherzustellenden Datei vorhanden ist, wird sie umbenannt.
7. Klicken Sie anschließend auf *eine der beiden* folgenden Schaltflächen:
   - Klicken Sie auf die Schaltfläche **Wiederherstellen**, um die Datei auf dem ursprünglichen Rechner wiederherzustellen.
   - Klicken Sie auf die Schaltfläche **Ziel auswählen**, um die Datei auf einem anderen Rechner mit kompatiblem Betriebssystem wiederherzustellen.
     - ✓ Ein Fenster mit einer Liste der verfügbaren Rechner mit kompatiblem Betriebssystem wird eingeblendet.
     - ✓ Sie können diese Liste anhand einer Rechner-ID oder Rechnergruppe filtern. Klicken

Sie anschließend auf die Schaltfläche **Aktualisieren**.

✓ Wählen Sie einen Rechner aus.

Wiederherstellung eines Backups von einem *Offline*-Rechner

Wenn der ursprüngliche Rechner *offline* ist, können Sie ein Backup auf einem anderen Rechner wiederherstellen.

1. Wählen Sie im mittleren Bereich der Seite 'Online-Backup > **Wiederherstellen**' eine *Offline*-Rechner-ID mit -Symbolen und *aktiviertem Text* aus.
   - Ein Fenster mit einer Liste der verfügbaren Rechner mit kompatiblem Betriebssystem wird eingeblendet.
   - Sie können diese Liste anhand einer Rechner-ID oder Rechnergruppe filtern. Klicken Sie anschließend auf die Schaltfläche **Aktualisieren**.
   - Wählen Sie einen Rechner aus.
2. Wählen Sie einen Ersatzrechner aus.
3. Wählen Sie in der Dropdown-Liste **Backup-Instanz auswählen** Datum und Uhrzeit eines vorhandenen Backups aus.
4. Klicken Sie auf **Arbeitsplatz**, um die Ordnerstruktur zu erweitern. Die Ordnerstruktur enthält die Ordner und Dateien, die Bestandteil der ausgewählten Backup-Instanz sind.
5. Wählen Sie die Ordner und Dateien aus, die Sie wiederherstellen möchten.
6. Markieren Sie gegebenenfalls die Option **Vorhandene Dateien überschreiben**.
7. Wählen Sie mit **Wiederherstellen auf** den Speicherort auf dem *Ersatz*rechner aus, auf dem das Backup wiederhergestellt werden soll. Wenn Sie dieses Feld leer lassen, werden die Dateien entsprechend des ursprünglichen Speicherpfads auf dem Ersatzrechner wiederhergestellt. Auf Wunsch können Sie ein anderes Verzeichnis auf dem Ersatzrechner auswählen. UNC-Pfade werden nicht unterstützt. Nach Angabe des Speicherortes können Sie unter folgenden Optionen auswählen:
   - **Datei ersetzen, wenn vorhanden** – Wenn am angegebenen Zielspeicherort eine Version der wiederherzustellenden Datei vorhanden ist, wird sie mit der wiederhergestellten Datei überschrieben.
   - **Datei umbenennen, wenn vorhanden** – Wenn am angegebenen Zielspeicherort eine Version der wiederherzustellenden Datei vorhanden ist, wird sie umbenannt.
8. Klicken Sie auf **Wiederherstellen auf <Rechner-ID>**, um die Dateien auf dem Ersatzrechner wiederherzustellen.

Verwalten

Data Backup > Wiederherstellung > Verwalten

Auf der Seite **Verwalten** können Sie Dateien und Ordner für ausgewählte Rechner-IDs aus dem Cloud-Speicher löschen. Wählen Sie im rechten Bereich eine oder mehrere Dateien oder Verzeichnisse aus. Klicken Sie unten auf der Seite auf die Schaltfläche **Löschen**.

Im Auswahlbereich der Backup-Instanz können Sie sehen, welche Dateien zum Zeitpunkt des angegebenen Backups gespeichert wurden. **Sämtliche Instanzen der ausgewählten Dateien werden vom Speicher gelöscht, unabhängig davon, welche Backup-Instanz ausgewählt ist.**

> **Hinweis:** Rechner-IDs werden auf dieser Seite nur angezeigt, wenn **Data Backup** darauf **installiert** *(siehe 11)* ist. Die Liste der auswählbaren Rechner-IDs basiert auf dem Rechner-ID-/Gruppen-ID-Filter und dem verwendeten Scope.

Übersicht

Data Backup > Speicher > Übersicht

Auf der Seite **Übersicht** werden Speicherstatistiken der einzelnen gesicherten Rechner-IDs angezeigt. Gezeigt werden Datum und Uhrzeit des letzten Backups, die *komprimierte* Größe des letzten Backups und die Gesamtgröße aller gespeicherten Dateien in *komprimiertem Zustand*.

> **Hinweis:** Rechner-IDs werden auf dieser Seite nur angezeigt, wenn **Data Backup** darauf **installiert** *(siehe 11)* ist. Die Liste der auswählbaren Rechner-IDs basiert auf dem Rechner-ID-/Gruppen-ID-Filter und dem verwendeten Scope.

Spalten

- **Rechner-ID** – Die Rechner-ID des verwalteten Rechners, von dem ein Backup erstellt wird.
- **Speicherserver** – Der von dieser Rechner-ID benutzte Speicherserver
- **Letztes Backup** – Datum und Uhrzeit des letzten Backups dieser Rechner-ID
- **Größe des letzten Backups** – Die komprimierte Größe des letzten Backups dieser Rechner-ID
- **Speicher-Übersicht** – Die komprimierte Größe aller Backups dieser Rechner-ID
- **Effizienzfaktor** – Das Verhältnis der ursprünglichen Größe des Backups zur komprimierten Größe dieser Rechner-ID (ausgedrückt als Vielfaches)
- **Wiederherstellungsrate** – Die durchschnittliche Geschwindigkeit, mit der Backups auf dieser Rechner-ID wiederhergestellt wurden.

Überblick

Data Backup > Speicher > Überblick

Die Seite **Überblick** enthält Speicherstatistiken, die zuerst nach privaten Speicherservern und dann nach Rechner-ID gruppiert angezeigt werden. Diese Statistiken zeigen die Anzahl der gespeicherten Dateien sowie die Größe der *ursprünglichen* und der *komprimierten* gespeicherten Dateien.

> **Hinweis:** Nur als **Data Backup**-Speicherserver definierte Rechner werden auf dieser Seite angezeigt. Die Liste der angezeigten Rechner basiert auf dem Rechner-ID-/Gruppen-ID-Filter und dem Scope des Benutzers.

Die für jeden Speicherserver angezeigten Spalten

- **Speicherserver** – Die Rechner-ID des Speicherservers
- **Wiederherstellungsdauer** – Die für die Wiederherstellung von Backups von diesem Speicherserver erforderliche Zeit.
- **Wiederherstellungsrate (MB/s)** – Die durchschnittliche Geschwindigkeit, mit der Backups von diesem Speicherserver wiederhergestellt wurden.
- **Anzahl der Dateien** – Die Anzahl der auf diesem Speicherserver gesicherten Dateien
- **Roh-Backup-Größe** – Die ursprüngliche Größe aller auf diesem Speicherserver gesicherten Dateien und Ordner
- **Tatsächliche Backup-Größe** – Die komprimierte Größe aller auf diesem Speicherserver gesicherten Dateien und Ordner
- **Effizienzfaktor** – Das Verhältnis der ursprünglichen Größe des Backups zur komprimierten Größe (ausgedrückt als Vielfaches)

Die für jeden Rechner angezeigten Spalten

- **Agent** – Die Rechner-ID des Agent-Rechners
- **Wiederherstellungsdauer** – Die für die Wiederherstellung von Backups auf diesem Agent-Rechner erforderliche Zeit
- **Wiederherstellungsrate (MB/s)** – Die durchschnittliche Geschwindigkeit, mit der Backups auf diesem Agent-Rechner wiederhergestellt wurden.
- **Anzahl der Dateien** – Die Anzahl der gesicherten Dateien dieses Agent-Rechners
- **Roh-Backup-Größe** – Die ursprüngliche Größe aller gesicherten Dateien und Ordner dieses Agent-Rechners
- **Tatsächliche Backup-Größe** – Die komprimierte Größe aller gesicherten Dateien und Ordner dieses Agent-Rechners
- **Effizienzfaktor** – Das Verhältnis der ursprünglichen Größe des Backups zur komprimierten Größe (ausgedrückt als Vielfaches)

Installieren/Entfernen

Data Backup > Konfigurieren > Installieren/Entfernen

Über die Seite **Installieren/Entfernen** wird nichts auf dem zu sichernden Agent-Rechner installiert, sondern die Verwaltung dieses Rechners durch **Data Backup** ermöglicht. Die Installation ist erforderlich, damit die Rechner-ID auf anderen **Data Backup**-Seiten angezeigt wird.

Unterstützte Betriebssysteme:

Kaseya Server

- Das Data Backup R8-Modul setzt VSA R8 voraus.

Anforderungen für verwaltete Rechner

- Microsoft Windows Server 2003, 2003 R2, 2008, 2008 R2, 2012, 2012 R2
- Microsoft Windows XP, Vista, 7, 8, 8.1
- Apple OS X 10.5 bis 10.9 – nur Intel

Anforderungen für private Speicherserver

- Microsoft Windows XP, Vista, 7, 8
- Microsoft Windows Server 2003, 2003 R2, 2008, 2008 R2, 2012
- Auf einem privaten Speicherserver muss ein Agent installiert sein.
- Achten Sie darauf, dass auf dem privaten Speicherserver ausreichend Speicherplatz vorhanden ist, um die Speicheranforderungen des Endpunkts zu erfüllen.

Backups werden über die Seite **Planen** *(siehe 4)* erstellt.

Aktionen

- **Installieren** – Aktiviert die **Data Backup**-Funktionalität auf ausgewählten Rechner-IDs.
- **Entfernen** – Deinstalliert die **Data Backup**-Funktionalität von ausgewählten Rechner-IDs.

> **Warnung:** Durch die Deinstallation werden auch alle dazugehörigen in der Cloud gespeicherten Backup-Daten gelöscht.

- **Automatisch aktualisieren** – Wenn dieses Kontrollkästchen aktiviert ist, wird der Seitenbereich automatisch alle fünf Sekunden aktualisiert.

Rechner-ID

Die Liste der angezeigten Rechner-IDs basiert auf dem Rechner-ID-/Gruppen-ID-Filter und den Rechnergruppen, zu deren Ansicht über 'System > Benutzersicherheit > Scopes' der Benutzer berechtigt ist.

Check-in-Status

Diese Symbole geben den Agent-Anmeldestatus jedes verwalteten Rechners an. Wenn Sie den Cursor über ein Anmeldesymbol bewegen, wird das Agent-Quick View-Fenster angezeigt.

- Online, aber in Wartestellung bis zum Abschluss des ersten Audits
- Agent online
- Agent online und Benutzer gegenwärtig angemeldet.
- Agent online und Benutzer gegenwärtig angemeldet, doch Benutzer seit mehr als 10 Minuten nicht aktiv
- Agent ist gegenwärtig offline
- Agent hat nie eingecheckt.
- Agent ist online, aber die Fernsteuerung wurde deaktiviert.
- Agent wurde ausgesetzt.

Installiert

Der **Data Backup**-Installationsstatus der einzelnen Rechner IDs

Backup-Profile

Data Backup > Konfigurieren > Backup-Profile

Auf der Seite **Backup-Profile** können Sie Konfigurationsprofile für das Backup verwalten. Jedes Backup-Profil besteht aus einem unterschiedlichen Satz aktivierter bzw. deaktivierter Backup-Optionen, darunter die für das Backup vorgesehenen Dateitypen und Dateispeicherorte. Ein- und Ausschlussregeln können nach Dateityp definiert werden. **Dateien und Verzeichnisse werden entsprechend einer festen Rangfolge ein- bzw. ausgeschlossen.** *(siehe 15)*

Änderungen an einem Profil wirken sich auf alle Rechner-IDs aus, denen dieses Profil zugewiesen wurde. Normalerweise benötigen verschiedene Typen von Rechnern unterschiedliche Backup-Profile. Es wird Ihnen ein Musterprofil bereitgestellt. Dieses Musterprofil kann zwar nicht geändert werden, aber Sie können es unter einem neuen Namen speichern und dann Änderungen an der Kopie vornehmen. Zu den Backup-Profiloptionen gehören Performance-Optionen zur Bandbreiten- und CPU-Einschränkung.

Backup-Profile sind optional, aber sehr zu empfehlen. Bei der einzigen anderen Methode für die Planung eines Backups müssen Sie Dateien einzeln auf einem Rechner auswählen. Backup-Profile werden mit der Profilauswahl rechts oben auf der Seite **Planen** *(siehe 4)* einem Rechner-ID-Konto zugewiesen.

Aufbewahrungsrichtlinie

- Backup-Daten der letzten 30 Tage werden im Online-Speicher aufbewahrt.
- Inkrementelle Backups werden nur gespeichert, wenn seit der letzten Speicherung Änderungen vorgenommen worden sind.
- Nach Speicherung von jeweils 30 inkrementelle Backups erfolgt das darauffolgende Backup als Spiegel-Backup (vollständig).
- Wenn ein inkrementelles Backup 80 % oder mehr der Größe der gesicherten Datei erreicht, wird ein Spiegel-Backup (vollständig) erstellt.
- Wenn sich eine Datei seit mehr als 30 Tagen nicht geändert hat, wird nur ihre letzte Version aufbewahrt.
- Wenn eine Datei vom Agent gelöscht wird, wird die letzte Version zeitlich unbegrenzt extern gespeichert, es sei denn, sie wird mithilfe der Funktion **Verwalten** *(siehe 9)* gelöscht.
- Für sowohl Cloud- als auch private Speicherung gilt, dass, wenn **Data Backup** von einem Endpunkt deinstalliert wird, alle Backup-Daten dieses Endpunkts vom Speicherserver gelöscht werden.

- Für Cloud-Speicherung gilt, dass, wenn der Kaseya-Agent vor **Data Backup** vom einem Endpunkt deinstalliert wird, die Daten auf dem Amazon S3-Server verbleiben und *Ihnen die Nutzung weiterhin in Rechnung gestellt wird*.

Aktionen

- **Neu** – Erstellt ein neues Profil.
- **Speichern** – Speichert die an einem ausgewählten Profil vorgenommenen Änderungen.
- **Speichern unter** – Speichert ein ausgewähltes Profil unter einem neuen Namen.
- **Umbenennen** – Benennt ein ausgewähltes Profil um.
- **Löschen** – Löscht ein ausgewähltes Profil.

Dateiregeln

> **Hinweis:** Geben Sie, wenn Sie Objekte in ein Profil einschließen bzw. davon ausschließen, ein Prozentzeichen (%) als erstes Zeichen ein, um eine Liste mit **Profilvariablen** *(siehe 14)* anzuzeigen. Nicht alle Profilvariablen gelten für OSX-Betriebssysteme.

Dateien und Ordner einschließen

Geben Sie an, welche Dateitypen eingeschlossen werden sollen.

- **Dateityp einschließen** – Geben Sie durch ein Leerzeichen getrennte Dateierweiterungen ein. Beispiel: `DOC TXT PDF HTML`
- **Ordner einschließen** – Geben Sie den Pfad eines Ordners ein, den Sie einschließen möchten.
- **Datei einschließen** – Geben Sie den vollständigen Pfad einer Datei ein, die Sie einschließen möchten.
- **Dateien ausschließen größer als <N> Megabyte** – Geben Sie die Größe in Megabyte ein.

Dateien und Ordner ausschließen

Dateien und Verzeichnisse werden entsprechend einer festen Rangfolge ein- bzw. ausgeschlossen. *(siehe 15)*

- **Dateityp ausschließen** – Geben Sie durch ein Leerzeichen getrennte Dateierweiterungen ein. Beispiel: `DOC TXT PDF HTML`
- **Ordner ausschließen** – Geben Sie den vollständigen Pfad des Ordners ein, den Sie ausschließen möchten.
- **Datei ausschließen** – Geben Sie den vollständigen Pfad der Datei ein, die Sie ausschließen möchten.

Leistung

- **Bandbreiteneinschränkung aktivieren** – Wenn Sie dieses Kontrollkästchen markieren, wird die Bandbreiteneinschränkung entsprechend den von Ihnen unten angegebenen Optionen aktiviert.
  - **Übertragung auf einen Anteil der gesamten Netzwerkverbindung begrenzen** – Wählen Sie den Prozentsatz der Netzwerkbandbreite aus bzw. geben Sie ihn ein, der Backups zugewiesen werden soll.
  - **Den ganzen Tag über einschränken/Im folgenden Zeitraum einschränken** – Wählen Sie aus, wann die Bandbreite tags- bzw. nachtsüber eingeschränkt werden soll.
- **CPU-Einschränkung aktivieren** – Wenn Sie dieses Kontrollkästchen markieren, wird die CPU-Einschränkung entsprechend den von Ihnen unten angegebenen Optionen aktiviert.
  - **CPU-Verwendung für Backup als Prozentsatz festlegen** – Begrenzt den **Data Backup** zugewiesenen Prozentsatz der CPU-Leistung.
  - **Den ganzen Tag über einschränken/Im folgenden Zeitraum einschränken** – Wählen Sie aus, wann die CPU-Leistung tags- bzw. nachtsüber eingeschränkt werden soll.

Profil gemeinsam nutzen

Sie können das Profil entweder als öffentlich kennzeichnen oder nur Ihrer Benutzerrolle zuweisen.

- **Öffentlich** – Alle Benutzer können dieses Profil einsehen, bearbeiten und nutzen.
- **Privat** – Zugriff auf dieses Profil ist auf Benutzer mit Master-Rolle und Benutzer beschränkt, die zu Ihrer Rolle gehören.

Lebensdauer-Richtlinie

Ist die Option **Selektive Lebensdauer** aktiviert, werden Dateien, die älter als ein angegebener Zeitraum sind, beim nächsten Backup aus dem *Speicher* gelöscht, wenn sie vom Backup ausgeschlossen oder von der Festplatte gelöscht wurden. Dies gewährleistet, dass selbst gelöschte Dateien für eine gewisse Zeit aufbewahrt werden und gleichzeitig der Gesamtspeicherplatzbedarf reduziert wird. Diese Option gilt für die Backups aller von diesem Profil verwalteten Agent-Rechner.

> **Warnung:** *Die Aktivierung dieser Funktion kann dazu führen, dass gespeicherte Backup-Versionen automatisch gelöscht werden!* Achten Sie daher darauf, dass Sie, wenn Sie diese Funktion aktivieren, Backups häufiger einplanen als den unter **Ablauf des Speichers** angegebenen Zeitraum.

- **Selektive-Lebensdauer-Richtlinie aktivieren** – Ist diese Option aktiviert, werden Dateien, die älter als der unter **Ablauf des Speichers** angegebene Zeitraum sind, beim nächsten Backup aus dem *Speicher* gelöscht, wenn sie vom Backup ausgeschlossen oder von der Festplatte gelöscht wurden.
- **Ablauf des Speichers (5–60 Tage)** – Die Standardeinstellung ist 30 Tage.

Wiederherstellungshorizont

Diese Option ist immer aktiviert. Vollständige und inkrementelle Backups, die älter als der Wiederherstellungshorizont sind, werden in eine einzige Backup-Instanz mit den Daten konsolidiert, die dem Wiederherstellungshorizont am nächsten liegen. Backup-Instanzen, die vor dem Datum des Wiederherstellungshorizonts liegen, werden entfernt. Gültige Werte für den Wiederherstellungshorizont liegen zwischen 15 und 120 Tagen.

- **Wiederherstellungshorizont (15–120 Tage)** – Die Standardeinstellung ist 30 Tage.

Anzahl inkrementeller Backups

Diese Option ist immer aktiviert. Der unter 'Anzahl inkrementeller Backups' eingegebene Wert kontrolliert, wie viele inkrementelle Backups zwischen vollständigen Backups einer Datei zugelassen sind. Dieser Wert wird auf Dateibasis angewendet. Sobald eine Datei die zulässige Höchstzahl inkrementeller Backups erreicht hat, wird ein vollständiger Backup ausgeführt.

- **Anzahl inkrementeller Backups (0–30)** – Die Standardeinstellung ist 30. Ist der eingestellte Wert 0, wird jedes Backup als vollständiges Backup ausgeführt.

Profilvariablen

Geben Sie, wenn Sie Objekte in ein Profil einschließen bzw. davon ausschließen, ein Prozentzeichen (%) als erstes Zeichen ein, um eine Liste mit *Profilvariablen* anzuzeigen. Nicht alle Profilvariablen gelten für OSX-Betriebssysteme. **Dateien und Verzeichnisse werden entsprechend einer festen Rangfolge ein- bzw. ausgeschlossen.** *(siehe 15)*

Windows OS

Benutzerumgebungsvariablen

- `%AppData%` – Das benutzerspezifische Anwendungsdatenverzeichnis
- `%Desktop%` – Das benutzerspezifische Desktop-Verzeichnis

- `%Favorites%` – Die in diesem Verzeichnis gespeicherten Favoriten des Benutzers
- `%LocalApplicationData%` – Das benutzerspezifische lokale Anwendungsdatenverzeichnis
- `%MyMusic%` – Das Verzeichnis 'Eigene Musik' des Benutzers
- `%MyPictures%` – Das Verzeichnis 'Eigene Bilder' des Benutzers
- `%Personal%` – Das Verzeichnis "Eigene Dokumente" des Benutzers
- `%MyDocuments%` – Das Verzeichnis 'Eigene Dokumente' des Benutzers
- `%UserProfile%` – Das Profil- bzw. Startverzeichnis des Benutzers
- `%Programs%` – Die Startmenüprogramme des Benutzers
- `%UserName%` – Der Anmeldename (nicht der vollständige Name) des Benutzers

Systemumgebungsvariablen

- `%CommonApplicationData%` – Das Anwendungsdatenverzeichnis aller Benutzer
- `%CommonDesktop%` – Das Desktop-Verzeichnis aller Benutzer
- `%CommonDocuments%` – Das Dokumentenverzeichnis aller Benutzer
- `%CommonProgramFiles%` – Das 'Gemeinsame Dateien'-Verzeichnis aller Benutzer
- `%CommonStartMenu%` – Das Startmenüelemente-Verzeichnis aller Benutzer
- `%WinDir%` – Das Verzeichnis, in dem Windows installiert ist.
- `%ComputerName%` – Der Name des Computers. Auf einer Domäne ist dies der qualifizierte Name.
- `%System%` – Das Verzeichnis, in dem die Systemdateien installiert sind.
- `%Profiles%` – Das Verzeichnis, in dem das System die Benutzerverzeichnisse abgelegt.
- `%ProgramFiles%` – Das Verzeichnis, in dem das System die Systemprogramme ablegt.

OSX

Benutzerumgebungsvariablen

- `%Desktop%` – Das `\Desktop`-Verzeichnis des Benutzers
- `%MyMusic%` – Das `\Musik`-Verzeichnis des Benutzers
- `%MyPictures%` – Das `\Bilder`-Verzeichnis des Benutzers
- `%MyDocuments%` – Das `\Dokumente`-Verzeichnis des Benutzers
- `%Programs%` – Das `\Bibliothek`-Verzeichnis des Benutzers
- `%UserName%` – Der Anmeldename (nicht der vollständige Name) des Benutzers

Systemumgebungsvariablen

- `%CommonProgramFiles%` – Das `\Bibliothek`-Verzeichnis
- `%WinDir%` – Das `\Bin`-Verzeichnis
- `%ComputerName%` – Der Name des Computers. Auf einer Domäne ist dies der qualifizierte Name.
- `%System%` – Das `\System`-Verzeichnis
- `%ProgramFiles%` – Das `\Anwendungen`-Verzeichnis

Ein- und Ausschließen von Dateien und Verzeichnissen

Data Backup setzt beim Ein- und Ausschließen von Dateien und Verzeichnissen die folgende

Rangordnung ein. Je niedriger die Zahl, desto höher die Priorität. Diese Ein-/Ausschluss-Prioritäten gelten für alle Kombinationen der beiden für den Ein- bzw. Ausschluss von Dateien und Verzeichnissen verwendeten Methoden:

- Auswahl von Verzeichnissen und Dateien über die Explorer-Struktur der Seite **Planen** *(siehe 4)*
- Über Benutzerprofile getroffene Auswahl auf der Seite **Backup-Profile** *(siehe 12)*

Typ des Profileintrags	Rangpriorität
Datei einschließen	1
Größe ausschließen: > X	2
Dateityp ausschließen*	3
Datei ausschließen	4
Ordner einschließen	5
Ordner ausschließen	6
Dateityp einschließen*	7

* Umgebungsvariablen funktionieren wie der Ein- bzw. Ausschluss von Dateitypen.

Hinweis: Siehe Beispiele in der **Knowledge Base** *(https://helpdesk.kaseya.com/entries/36140563)*.

Meldungen

Data Backup > Konfigurieren > Meldungen

Die Seite **Meldungen** gibt in Reaktion auf erfolgreiche bzw. fehlgeschlagene **Data Backup**-Ereignisse Meldungen aus.

Hinweis: Rechner-IDs werden auf dieser Seite nur angezeigt, wenn **Data Backup** darauf **installiert** *(siehe 11)* ist. Die Liste der auswählbaren Rechner-IDs basiert auf dem Rechner-ID-/Gruppen-ID-Filter und dem verwendeten Scope.

So erstellen Sie eine Meldung:

1. Aktivieren Sie beliebige dieser Kontrollkästchen, um bei Auftreten einer Meldungsbedingung die entsprechenden Aktionen auszuführen:
   - **A**larm erstellen
   - **T**icket erstellen
   - **S**kript ausführen
   - **E**-Mail-Empfänger
2. Legen Sie weitere E-Mail-Parameter fest.
3. Wählen Sie eine der folgenden Optionen aus:
   - `Meldung bei 'Backup abgeschlossen'`
   - `Meldung bei 'Backup mit Ausnahmen abgeschlossen'`
   - `Meldung bei 'Backup übersprungen'`
   - `Meldung bei 'Backup-Speicherung verwendet X GB'`
   - `OnlineBackupMonitorService-Fehler`
4. Markieren Sie die Rechner-IDs, auf die die Meldungseinstellungen angewendet werden sollen.

5. Klicken Sie auf **Anwenden**, um die Meldungseinstellungen auf die ausgewählten Rechner-IDs anzuwenden.

So kopieren Sie Meldungseinstellungen:

1. Markieren Sie `alle Einstellungen kopieren von`.
2. Klicken Sie auf **(Klicken Sie zum Auswählen)**, um den von **Data Backup** verwalteten Rechner auszuwählen, dessen Meldungseinstellungen ausgewählt werden sollen.
3. Markieren Sie die Rechner-IDs, auf die die Meldungseinstellungen angewendet werden sollen.
4. Klicken Sie auf **Anwenden**, um die Meldungseinstellungen auf die ausgewählten Rechner-IDs anzuwenden.

Alarm erstellen

Wenn diese Option aktiviert ist und eine Meldungsbedingung auftritt, wird ein Alarm erstellt. Alarme werden in Monitor > Dashboard-Liste, Monitor > Alarmübersicht und Info Center > Reporting > Berichte > Protokolle > Alarmprotokoll angezeigt.

Ticket erstellen

Wenn diese Option aktiviert ist und eine Meldungsbedingung auftritt, wird ein Ticket erstellt.

Agent-Verfahren ausführen

Wenn dies aktiviert ist und eine Meldungsbedingung auftritt, wird ein Agent-Verfahren ausgeführt. Sie müssen auf den Link **Agent-Verfahren auswählen** klicken, um ein auszuführendes Agent-Verfahren zu wählen. Sie können das Agent-Verfahren optional anweisen, in einem angegebenen Bereich von Rechner-IDs zu laufen, indem Sie auf den Link **diese Rechner-ID** klicken. Diese angegebenen Rechner-IDs müssen nicht der Rechner-ID aus der Meldungsbedingung entsprechen.

E-Mail senden an

Ist diese Option aktiviert und es tritt eine Meldungsbedingung ein, werden E-Mails an die angegebenen E-Mail-Adressen gesendet.

- Wenn das Optionsfeld **Zur aktuellen Liste hinzufügen** aktiviert ist, werden beim Klicken auf **Anwenden** die Meldungseinstellungen angewendet und die angegebenen E-Mail-Adressen hinzugefügt, ohne dass die zuvor zugewiesenen E-Mail-Adressen entfernt werden.
- Wenn das Optionsfeld **Liste ersetzen** aktiviert ist, werden beim Klicken auf **Anwenden** die Meldungseinstellungen angewendet und die zuvor zugewiesenen E-Mail-Adressen durch die angegebenen E-Mail-Adressen ersetzt.
- Wenn Sie auf **Entfernen** klicken, werden alle E-Mail-Adressen entfernt, **ohne dass irgendwelche Meldungsparameter geändert werden**.
- E-Mails werden vom Kaseya Server direkt an die in der Meldung angegebene E-Mail-Adresse gesendet. Den **Absender** können Sie über 'System > Ausgehende E-Mail' festlegen.

Check-in-Status

Diese Symbole geben den Agent-Anmeldestatus jedes verwalteten Rechners an. Wenn Sie den Cursor über ein Anmeldesymbol bewegen, wird das Agent-Quick View-Fenster angezeigt.

- Online, aber in Wartestellung bis zum Abschluss des ersten Audits
- Agent online
- Agent online und Benutzer gegenwärtig angemeldet.
- Agent online und Benutzer gegenwärtig angemeldet, doch Benutzer seit mehr als 10 Minuten nicht aktiv
- Agent ist gegenwärtig offline
- Agent hat nie eingecheckt.
- Agent ist online, aber die Fernsteuerung wurde deaktiviert.
- Agent wurde ausgesetzt.

Rechner.Gruppen-ID

Die Liste der angezeigten Rechner.Gruppen-IDs basiert auf dem Rechner-ID-/Gruppen-ID-Filter und den Rechnergruppen, die der Benutzer befugt ist, mithilfe von System > Benutzersicherheit > Scopes anzuzeigen.

Name der Meldung

Listet die für die einzelnen Rechner-IDs möglichen Meldungen auf.

Antworten

Der jeder Meldung der einzelnen Rechner-IDs zugewiesene ATSE-Antwortcode:

- A = **A**larm erstellen
- T = **T**icket erstellen
- S = **S**kript ausführen
- E = **E**-Mail-Empfänger

Auszuführendes Agent-Verfahren

Das Agent-Verfahren, das ausgeführt werden soll, wenn diese Meldungsbedingung eintritt.

Agent-Verfahren auszuführen auf

Die Rechner-ID, auf der das Agent-Verfahren ausgeführt wird, wenn diese Meldungsbedingung eintritt.

E-Mail an

Eine kommagetrennte Liste von E-Mail-Adressen, an die Benachrichtigungen gesendet werden.

Privater Speicher

Data Backup > Konfigurieren > Privater Speicher

Auf der Seite **Privater Speicher** werden Agent-Rechner als private Speicherserver konfiguriert. Der private Speicherserver muss sich nicht im selben lokalen Netzwerk wie der zu sichernde Rechner befinden. Ein privater Speicherserver kann auf ein lokales Laufwerk oder einen UNC-Pfad zu einem externen Speicher wie beispielsweise einem NAS-Gerät verweisen. Sie brauchen nur einen DNS-Namen oder eine IP-Adresse, Portnummer sowie ein lokales Laufwerk und ein Ordnerverzeichnis angeben. Für die Dateispeicherung gibt es keine Größenbeschränkungen. Für private Speicherserver fallen keinen diesbezüglichen Lizenzgebühren an. **Data Backup** muss auf dem als privater Speicherserver vorgesehenen Rechner nicht installiert werden.

> **Hinweis:** Die Liste der auswählbaren Rechner-IDs basiert auf dem Rechner-ID-/Gruppen-ID-Filter und dem verwendeten Scope.

So konfigurieren Sie einen privaten Speicher

1. Wählen Sie im mittleren Bereich einen Rechner aus.
2. Geben Sie die folgenden Speicher-Anmeldedaten ein:
   - **IP-Adresse** – Die IP-Adresse, über die mit dem Speicherserver kommuniziert werden kann.
   - **Port** – Der Eingangsanschluss, über den mit dem Speicherserver kommuniziert werden kann. Geben Sie eine beliebige Portnummer an, die nicht von einem anderen Prozess belegt ist.
   - **Backup-Speicherort** – Der Pfad zu dem Verzeichnis und Ordner, die für das Speichern von Backups auf einem Speicherserver verwendet werden. Der Ordnerpfad muss bereits auf

dem Speicherserver vorhanden sein, da er nicht automatisch erstellt wird. Beispiel: `c:\databackups`

Spalten

- **Rechner-ID** – Der im VSA verwendete Name des Agents dieses Rechners.
- **Speicher** – Wird ein Serversymbol angezeigt, wird dieser Rechner als privater Speicherserver verwendet.
- **Verfügbare Kapazität** – Der gesamte freie Speicherplatz auf der Rechner-ID
- **Betriebszeit** – Die Zeit in Prozent, die ein verwalteter Rechner in Betrieb war.

Kaseya Cloud Storage

Data Backup > Konfigurieren > Kaseya Cloud Storage

Kaseya nutzt die Leistungsstärke der von Amazon S3 bereitgestellten Speicherlösung aus, um das Speichern Ihrer Daten in der Cloud für Sie so einfach und sicher wie möglich zu machen. Amazons Speicher bietet Ihren Daten ein extrem zuverlässiges und robustes Repository, damit Sie sich nicht nur auf die Verfügbarkeit Ihrer Daten, sondern auch auf die Compliance mit wichtigen Branchenstandards verlassen können.

Ihnen stehen zwei Optionen zur Wahl:

- **Speicher testen**
- **Gebührenpflichtigen Speicher verwenden**

Speicher testen

Sie können **Kaseya Cloud Storage** sofort ausprobieren. Die Testzeit beginnt mit dem ersten Backup. Wenn Sie auf die Schaltfläche **Speicher testen** klicken, wird die Amazon S3-Speicheroption den Optionen **Speicherserver anwenden** auf der Seite **Planen** *(siehe 4)* hinzugefügt.

Während der Testzeit können Sie beliebig viele Daten speichern. Am Ende der Testzeit werden Ihre Daten auf sichere Weise gelöscht, es sei denn, Sie entschließen sich, Ihren Speicher zu aktivieren und in ein gebührenpflichtiges Konto umzuwandeln. Bei Aktivierung Ihres Kontos können Sie die bereits gespeicherten Daten weiterhin verwenden.

Gebührenpflichtigen Speicher verwenden

Um gleich bei **Kaseya Cloud Storage** einzusteigen, müssen Sie nur Ihr Konto mit einer Kreditkarte aktivieren. Ihre Kreditkarte wird erst belastet, wenn Sie Daten in der Cloud speichern.

Für die Aktivierung müssen Sie sich bei Ihrem **Kaseya-Helpdesk** *(https://helpdesk.kaseya.com/home)*-Konto anmelden und eine Kreditkarte registrieren. Wenn Sie noch kein Kaseya-Konto besitzen, benötigen Sie Ihre Kunden-ID und müssen den Kundendienst anrufen, um die Anmeldeformalitäten zu erledigen.

> **Hinweis:** Um Gebühren für **Kaseya Cloud Storage** zu vermeiden, wenn Sie diesen Dienst nicht länger benötigen, deinstallieren Sie zuerst alle Komponenten von Geräten, die Kaseya Cloud Storage verwenden, bevor Sie anschließend Kaseya-Agents (z. B. Kaseya-Backup-Agents) deinstallieren. Dadurch werden die in der Cloud gespeicherten Daten am Ende des Abrechnungszeitraums gelöscht, und alle mit diesen Daten verbundenen Gebühren entfallen. Deinstallieren Sie jedoch den Kaseya-Agent zuerst, werden die Daten nicht aus der Cloud entfernt. Da das Speichersystem in diesem Fall davon ausgeht, dass Sie die Daten behalten möchten, werden Ihnen weiterhin Gebühren für alle vorher gespeicherten Daten angerechnet.

Datensicherung-Zusammenfassung

Info Center > Reporting > Berichte > Audit - Datensicherung-Zusammenfassung

- *Wird nur angezeigt, wenn das Data Backup-Zusatzmodul installiert ist.*

Mit der Berichtsdefinition **Datensicherung-Zusammenfassung** wird ein zusammenfassender Bericht der **Data Backup**-Aktivitäten nach Rechner-ID generiert.

Konfigurieren Sie Ihre Berichtsoption unter Verwendung der folgenden Parameter:

Zeitauswahl

- **Zeitbereichstyp auswählen** – Filtert Daten nach einem bestimmten Typ von Datumsbereich.
- **Anzahl der Tage** – Diese Option ist nur anwendbar, wenn `Letzte N Tage` als Zeitbereichstyp ausgewählt ist.
- **Benutzerdefinierte(s) Startdatum/-zeit** – Diese Option ist nur anwendbar, wenn `Festgelegter Bereich` als Zeitbereichstyp ausgewählt ist.
- **Benutzerdefinierte(s) Enddatum/-zeit** – Diese Option ist nur anwendbar, wenn `Festgelegter Bereich` als Zeitbereichstyp ausgewählt ist.

Parameter

- **Rechner ohne Daten miteinbeziehen** – Bei Aktivierung dieses Kontrollkästchens werden Rechner ohne Backups mit einbezogen.
- **Detail anzeigen** – Bei Aktivierung dieses Kontrollkästchens werden alle Backup-Aktivitäten für einen Rechner angezeigt. Bei Nichtaktivierung wird nur die letzte Backup-Aktivität angezeigt.

Datensicherungsnutzung im Zeitverlauf

Info Center > Reporting > Berichte > KOB - Datensicherungsnutzung im Zeitverlauf

- *Wird nur angezeigt, wenn das Data Backup-Zusatzmodul installiert ist.*

Mit der Berichtsdefinition **Datensicherungsnutzung im Zeitverlauf** wird ein Bericht der **Data Backup**-Nutzung nach Zeitperiode generiert.

Konfigurieren Sie Ihre Berichtsoption unter Verwendung der folgenden Parameter:

Zeitauswahl

- **Zeitbereichstyp auswählen** – Filtert Daten nach einem bestimmten Typ von Datumsbereich.
- **Anzahl der Tage** – Diese Option ist nur anwendbar, wenn `Letzte N Tage` als Zeitbereichstyp ausgewählt ist.
- **Benutzerdefinierte(s) Startdatum/-zeit** – Diese Option ist nur anwendbar, wenn `Festgelegter Bereich` als Zeitbereichstyp ausgewählt ist.
- **Benutzerdefinierte(s) Enddatum/-zeit** – Diese Option ist nur anwendbar, wenn `Festgelegter Bereich` als Zeitbereichstyp ausgewählt ist.

Parameter

- **Rechner ohne Daten miteinbeziehen** – Bei Aktivierung dieses Kontrollkästchens werden Rechner ohne Backups mit einbezogen.
- **Zeitperiode auswählen** – `Täglich`, `Wöchentlich`, `Monatlich`, `Vierteljährlich`, `Jährlich`.
- **Auslastungstyp auswählen** – `Spitzenauslastung anzeigen`, `Durchschnittliche Auslastung anzeigen`.

Inhaltsverzeichnis